AEGIS VENTURES | 2024. 6. 27

bitSmiley Review

- **목적**: Bitcoin Blockchain 기반으로 발행된 DEFI Platform
  (약어: Fintergra, Fintech + Integra)
- **Type**: DEFI (Stablecoin, P2P Lending, P2P Borrowing, Insurance)
- **Token Type**: bitUSD
- **Protocol**: bitRC-20 (UXTO, Inscription)

■ TLDR

- Bitcoin을 담보로 한 bitUSD 발행 지원
- 유동성이 높은 Bitcoin 혹은 bitRC-20 프로토콜로 발행된 Token을 담보로 하여 Lending/Borrowing 지원
- Lending/Borrowing을 보완하기 위한 목적으로 Insurance 서비스 지원
- BitInsurance에서 발행된 채권 상당액은 Pooling하여 CDS 방식으로 NFT 판매
- **(추가)** 기한 내 미상환 시 이에 따른 Auction 적용

Index

Ⅰ. Bitcoin & Smart Contract

비트코인은 Script라는 스택 데이터 구조를 가진 단순한 언어로 만들어진 PoW 합의 알고리즘을 가진 블록체인입니다. 해당 블록체인 내에서 발생하는 하나의 활동(Transaction)은 각각 구분되는 블록에서의 Transaction Input과 UTXO(Unspent Transaction Output) 및 이에 대한 트랜잭션을 승인하는 퍼블릭/프라이빗 키로 구성됩니다. 단순한 구조로 짜인 코드는 효율적으로 상태 변화에 대한 기록을 통해 원장으로의 기능을 수행하였지만, 1) 시스템의 안전성을 위해 Loop문을 지원하지 않아 복잡하고 다양한 계약구조를 담기 어려웠고, 2) PoW와 블록 사이즈 제한으로 인한 낮은 처리속도 3) Account 기반이 아닌 UTXO 형태의 잔고증명으로 인한 제한된 인터페이스 등의 문제를 포함하고 있었습니다.

이에 대한 해결책으로 등장한 것이 이더리움이었습니다. 초기 이더리움은 Account 기반의 개별 Wallet 및 Loop문, ERC-20 프로토콜 기반의 토큰 발행을 지원하여, 단순한 원장으로의 기능뿐만 아니라 코드 기반의 다양한 계약구조(이하 “스마트 컨트랙트”)를 담을 수 있도록 하였습니다. 이더리움이 지원하는 편리한 UI 및 스마트 컨트랙트는 이더리움 블록체인을 기반으로 현실에 적용 가능한 다양한 DApp 개발을 촉진시켰습니다. 이는 이후 NFT/DEFI/Validator 등 다양한 사업분야로 확장되게 됩니다.

이와 같은 성격을 가진 비트코인은 전송의 수단, 거래소 내 거래를 위한 단위로 시장 내에서 입지를 굳혔으나, 비트코인을 기반으로 하는 파생된 생태계는 Mining이나 제한된 실물시장에서의 거래 수단 및 가치저장 수단으로 그 범위가 제한되었습니다.

II. Existing crypto service overview

Bitcoin Layer2 v. Inscription (BRC-20)

비트코인의 한계를 극복하기 위해 제안된 것은 "Inscription", "Layer2"였습니다.

Inscription은 비트코인 블록체인 내에서 해결하기 위한 제안이었습니다. Inscription 트렌드는 2017 세그윗(Segwit)과 2021년경 진행된 탭루트(Taproot)라는 서명 방식의 개선에 그 기반을 두고 있습니다. 두가지 포크의 결과로 각 비트코인의 블록크기는 동일하되 필요 없는 데이터를 제거함으로써 저장 효율성을 개선하였고, MAST(Merklized Abstract Syntax Tree)를 통해 다수의 조건문에 대한 전체 검증 없이도 필요한 조건문만을 신속하게 처리하여 대량의 계약 처리도 가능하게 했습니다. Inscription은 증가된 저장효율성/속도 등을 통해 단일 블록에 식별가능한 별도의 데이터를 저장하여 다른 기능들을 구현합니다.

Layer2는 위의 한계를 비트코인 블록체인 외에서 해결하기 위한 제안이었습니다. Layer2에서는 메인체인(온체인)과 구분되는 별도의 오프체인을 구성하여 메인체인에는 결과에 대한 기록만을 수행하고, 대량연산 혹은 스마트 컨트랙트 같은 기능이 필요한 행위는 메인체인 밖에서 수행합니다. 이런 행위를 통해 비트코인의 작은 블록사이즈로 인한 한계를 개선할 수 있고, 더 나아가 부가적인 기능 또한 구현할 수 있습니다.

현재 관련 프로젝트들은 아래와 같은 것들이 있습니다.

구분	프로젝트명	Ticker	Smart Contract	Language	EVM-Compatible	Throughput (TPS)
Inscription	Ordinals	-	미지원	Script	X	7 ~ 10
		생성된 블록에 사토시 숫자를 부여하고, 사토시 상에 이미지를 Inscribing한 후 콜하여 자료를 열람하는 프로토콜				
Layer2 & Sidechain	Lightning network	-	미지원	Script	X	Fast
		(사이드체인) Commitment Tx/Funding Tx 스크립트를 응용한 빠른 속도의 P2P 거래지원				
	Stacks	STX	지원	Clarity	O	19
		(Layer 2) 스마트 컨트랙트를 지원하는 활성도가 높은 PoX 합의구조의 비트코인 Layer 2				
	Rootstock	RBTC	지원	Solidity	O	10 ~ 20
		(사이드체인) EVM을 지원하며 비트코인을 락업함으로써 이에 쌍대되는 RBTC를 생성, 사이드체인 상에서 스마트 컨트랙트 지원				
	Liquid	L-BTC	지원	Simplicity	X	7~10
		(사이드체인) 자산을 담보로 하여 체인 내에서 운용할 수 있는 사이드체인				

● Inscription 프로젝트

A) Ordinals

Ordinals는 비트코인 세그윗과 탭루트 소프트포크 이후 저장공간 및 단위 스크립트 크기 제한의 완화 이후 등장한 프로토콜로 BRC20의 기초가 됩니다. Ordinals는 비트코인 특유의 기능 제한으로 인한 스마트 컨트랙트 미지원의 한계를 오더링 방식으로 일부 해결합니다. 블록 생성 시점에 따라 오더링을 하고, 오더링을 수행한 사토시 상에 특정 데이터(Image, txt 등)를 JSON의 형태로 Inscribing하는 과정을 거칩니다.

위 과정 중 이미지와 같은 큰 용량을 차지하는 데이터를 저장하는 과정 중 수수료 문제가 있었으나, Recursive Inscription을 통해 특정 데이터를 쪼개 저장하는 방식의 접근은 더 효율적인 Inscription을 가능하도록 하였습니다.

● Layer2 프로젝트

A) Lightning Network

Lightning Network는 Funding Transaction과 Commitment Transaction 기능을 통해 구현한 오프체인 방식의 신속한 거래 방법을 제안했습니다. Funding Tx에 일정량의 비트코인을 예치하고 이를 Commitment Tx를 통해 수령해가는 구조에 기반하여 Multi-Hop Hasehd TimeLock Contract(이하 “HTLC”)를 이용한 다자간의 빠른 거래속도를 달성하였습니다. 이를 통해 블록사이즈 및 블록생성주기에 구애받지 않는 높은 거래 속도를 확보할 수 있었습니다.

B) Stacks

Stacks는 Clarity로 짜인 PoX 합의 알고리즘을 가진 블록체인입니다. Stakcs는 비트코인과 구분되는 별개의 블록체인을 구성하나, 최종적으로 블록체인과 Anchoring 되어 발생한 활동을 비트코인의 블록에 기록(Settlement)합니다. 또한 스택스는 가이아라고 하는 별도의 오프체인 스토리지 시스템을 사용하며 블록체인에 키값만을 저장하여 블록사이즈 문제를 해결하였습니다. 하지만 실질적으로 파이널리티의 단계에서 Settlement의 행위가 이루어져야 개별 활동이 주체인인 비트코인 블록체인에 저장되므로 비트코인의 Throughput에 제약을 받게 된다는 한계가 있습니다.

C) Rootstock

RootStock은 EVM-Interoperation을 지원하는 비트코인의 사이드체인입니다. RootStock은 RVM 가상머신을 통한 이더리움과 Interoperation이 가능하다는 특이점이 있으며, EVM 호환성에 따라 스마트 컨트랙트를 RootStock내에서 사용할 수 있다는 특이점이 있습니다. 이를 통해 비트코인의 스마트 컨트랙트의 한계를 개선하였지만, 내부에서 발생하는 활동을 파이널리티 단계에서 번들링하여 비트코인 블록에 기록하므로 비트코인의 Throughput에 제약을 받게 된다는 한계가 있습니다.

D) Liquid

Liquid는 비트코인의 사이드체인으로, 일정량의 비트코인을 예치하고 예치한 비트코인에 페어링된 L-BTC를 발행하는 방법을 채택하여 전송속도를 개선하였습니다. 하지만, 합의 컨센서스가 컨소시엄 형태의 블록체인을 띄고 있어 실질적인 비트코인의 본래의 취지와는 다르다는 한계가 있습니다.

● 비트코인 Layer 2의 DApps

비트코인 Layer 2의 Dapp 생태계는 스택스에 집중되어 있습니다. 이는 스택스가 EVM을 지원한다는 점과 최종 Settlement 시점에 비트코인에 그 결과를 저장하나, 이전에 합의에 따라 스택스 자체에서 Settlement를 진행할 수 있으므로 Layer2 내에서는 빠른 정산을 할 수 있다는 점에 있습니다. 아래는 Stacks에서 운영 중 혹은 예정인 대표적인 DEFI Dapp들입니다.

A) 알렉스 (Stacks, DEFI)

알렉스는 스택스 기반 DEFI-Protocol입니다. 알렉스는 BRC-20를 지원하며 EVM 형태로 스택스 기반의 비트코인 보안성뿐만 아니라 이더리움의 스마트 컨트랙트 역시 지원하는 구조의 서비스입니다. 알렉스에서는 Swap, Trade, Kickstart, Bridge의 기능을 지원합니다.

B) Hermetica (Stacks, DeFi)

Hermetica는 비트코인 DEFI Protocol(Option)입니다. Hermetica는 비트코인과 단기 선물 공매도 포지션을 합성하여 USDh를 생성합니다. USDh를 Stake할 경우 중앙화 거래소의 Perp 숏 포지션에서 발생하는 Funding Fee를 대가로 지급하는 구조를 가지고 있습니다.

C) StakingDAO (Stacks, DeFi-LST)

StakingDAO는 스택스 LST Protocol입니다. StakingDAO에서는 스택스를 스테이킹하여 스택스 자체에서 발생하는 Rewards를 얻습니다. 또한 스테이킹한 자들은 이에 대한 증표로 Liquid Staking Token을 부여받습니다. 여기서 발생한 유동성을 통해 Yield Farming 등 기타 스택스 상의 다른 DEFI 서비스에 LST를 사용할 수 있습니다.

Ⅲ. bitSmiley review

bitSmiley Details

bitSmiley는 비트코인의 Inscription 기능을 활용하여 기획된 프로젝트입니다. bitSmiley는 DEFI Protocol로 1) Stablecoin인 bitUSD의 발행 2) bitRC-20 기반의 Token 발행 3) P2P Lending & Borrowing 등을 지원합니다.

bitSmiley의 프로토콜 명칭은 bitRC-20로 JSON 형태로 기입되며 Inscription과 같은 방법을 채택하여 “Mint”, “Burn”, “Transfer” 등을 지원합니다. BitSmiley는 bitRC-20을 이용하여 최초 발행자산으로 bitUSD를 발행합니다. bitUSD는 1달러에 페깅된 토큰으로 비트코인을 예치하고 이를 담보로 발행되는 토큰입니다. 이는 과잉담보의 특성을 가지고 있으므로 비트코인의 가격이 유지된다면 안정적으로 운영될 수 있습니다. 하지만 발행 과정 이후 비트코인 가격이 하락할 경우 bitUSD가 담보로 하는 비트코인의 가치가 하락할 수 있으며, 본 경우 프로토콜 기반 경매 등을 통하여 bitUSD의 담보금액을 보완합니다.

기록된 오디널스 토큰을 기반으로 하여 bitSmiley의 이용자들은 Lending과 Borrowing을 수행합니다. 이는 스마트 컨트랙트와 같은 Pool 기반의 기능이 아니므로 Peer to Peer의 호가제시와 승낙의 절차로 이루어집니다. 이는 낮은 유동성의 문제를 갖습니다.

bitRC-20 토큰의 차용인은 비트코인 혹은 BitRC-20 프로토콜로 발행된 가치있는 토큰을 담보로 하여 Token을 차입할 수 있으며 대여자에게 이에 대한 이자로 일정량의 Token을 지급합니다. 블록체인 기반의 P2P Lending 서비스의 경우 차용인이 담보를 통해 Token을 Lending하였다고 하더라도 상환을 강제할 수 없다는 특징을 가지고 있습니다. 이는 대출자로 하여금 상환미이행의 리스크에 노출되는 문제를 야기할 수 있습니다.

또한 bitSmiley의 독특한 서비스는 BitInsurance입니다. Bitinsurance는 민간 보험상품을 거래할 수 있는 채널을 열어 대여자가 자신이 보유한 BitRC-20 기반의 토큰 가격의 변동을 보완할 수 있는 보험상품을 구매할 수 있습니다.

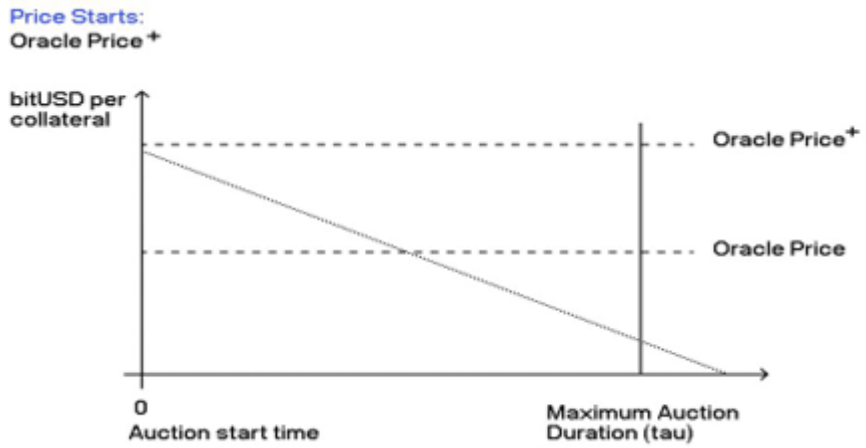
1) Product Detail

Business Model

bitSmiley은 DAO의 구조로, 다양한 이해관계인을 기반으로 하는 Economic Governance Committee로 구성되어 있습니다.

bitUSD

비트스마일리 옥션 구조



bitSmiley의 주된 프로덕트로 비트코인을 담보로 발행되는 USD입니다. bitUSD의 특징은 과담보형 USD로 초기 발행시점에 1) bitUSD의 수량이 결정되고 2) 담보하는 비트코인의 가격변동에 대한 Liquidation Price가 결정됩니다.

담보로 제공된 비트코인은 추후 가격변동에 따라 기존에 결정된 Liquidation Price의 임계점에 도달할 경우 청산절차로 들어가게 되고, 청산절차에 들어간 비트코인은 더치옥션(Dutch Auction)에 따른 경매절차를 진행하여 분배되게 됩니다.

독특한 방식은 청산의 과정에 Liquidator가 개입한다는 점입니다. Liquidation Price에 도달한 계약에 대해서 Liquidator는 비트코인의 경매를 진행하게 되고, 이 과정에서 낙찰가격과 시장가격에서 발생하는 차액 상당은 Liquidator와 프로토콜이 분배받아 수익화 합니다. 이 중 프로토콜 분배액 상당은 풀에 적립되어 안전기금으로 기능합니다. BitUSD와 관련된 활동이 증가할수록 청산과 관련된 안전자금이 증가하므로 시스템의 안정성은 높아집니다.

BitLending

Bitlending은 BitSmiley의 P2P Lending Protocol입니다. 각 플레이어는 자신의 비트코인 혹은 bitRC-20 토큰을 담보로 하여 제 3자로부터 비트코인 혹은 bitRC-20의 대출이 가능합니다. 하지만 기존의 DEFI 구조와 다르게 BitSmiley가 비트코인을 기반으로 이루진 프로젝트라는 점에서 두 가지 한계가 존재합니다.

첫번째로 비트코인 합의 알고리즘의 블록생성시간(10분) 문제로 인하여 거래의 내역이 정산(Settlement)되기까지 상당한 시간이 소요된다는 점입니다. 이는 대여 요청에 따른 승낙시점과 실제 집행시점 및 정산시점까지의 차이를 발생시킵니다. 이런 시간 갭은 체결 시점에서 집행시점까지의 가격 이격을 발생시킵니다. 이에 따라 단시간 내 급격한 가격변동의 익스포져에 개별 참가자는 노출될 수 있는 한계가 있습니다.

두번째로 Inscription의 한계로 다자간 Pool 기반 Lending을 지원하지 않는다는 한계가 있습니다. 이는 청약과 승낙의 방식으로 이루어지기 때문에 대여자 혹은 차입자는 자신이 원하는 수량을 차입하기 어렵습니다. 충분한 유동성이 없을 경우, 원하는 수량의 Lending을 수행하기 위해서는 많은 컨트랙트 생성 활동이 필요할 수 있습니다.

BitInsurance – 기본

Bitinsurance는 BitLending에서의 상환 및 익스포져에 대한 솔루션으로, 플랫폼 상에서 이루어진 담보대여 계약에 대한 민간형 보험 서비스입니다. Bitlending을 통해 이루어진 계약에 대해 비트코인 기반의 차입자는 청산의 위험에, 대여자는 미상환 리스크에 노출되어 있습니다.

Bitinsurance의 프로토콜은 BitLending에 참가하는 대여자와 차입자를 위한 보험상품을 제공합니다. 비트코인 담보대출자에게는 비트코인 가격 하락에 따른 청산을 방지하고, 대여자에게는 미상환에 따른 보전을 시도합니다.

bitSmiley가 제공하는 Bitinsurance에서 민간 보험자의 보험수수료 결정 모형은 Extreme Value Theory, T-Copula 방법에 따릅니다. 두 모형은 기후, 재난 등과 같은 통상적으로 발생할 가능성이 낮은 사건들에 대해 다루며 이로 인해 발생하는 손실 규모를 추정하는 보험 모형에 자주 사용되는 것입니다. 각 모형은 특정 사건의 발생과 그로 인해 연관되는 다양한 변인들의 관계성에 주목하여 모수를 추정합니다.

이는 비트코인이나 bitRC-20 계통의 가상자산 등과의 가격 연관성 등에 대한 통계를 제공하므로, 가상자산과 같은 변동성이 큰 자산들에 대한 보험 가격 추정에 유용할 수 있습니다.

아래는 간략한 Extreme Value Theory와 T-Copula에 대한 설명입니다.

1) Extreme Value Theory

Extreme Value Theory는 확률적으로 발생할 가능성이 매우 낮은 극단값들의 분포를 모델링하는 통계적인 방법입니다. 보험에서 대표적으로 사용되는 극단치 모형은 두가지입니다. 하나는 Block Maxima와 다른 하나는 Peaks Over Threshold(POT) 모형입니다. Block Maxima의 경우 기간별 극값에 대한 모형이고, POT의 경우에는 임계치 이상의 값들에 대한 모형입니다.

bitSmiley의 손실 예측 모형에는 상기 두 모형을 모두 사용합니다. Block Maxima를 통해서는 Generalize Extreme Value(GEV) 분포를 이용하여 적은 빈도의 데이터를 추정하고 POT를 통해서는 Generalized Pareto Distribution(GPD)를 통해 고빈도의 데이터에 대한 추정을 수행합니다.

각 두 모델을 사용하는 것은 각각 다음의 특징이 있습니다.

Block Maxima에서는 데이터 구간별로 극단에 있는 값 만을 보기 때문에 데이터를 단순화하기 용이합니다. Block Maxima에서 사용하는 Generalized Extreme Value(GEV)[1] 방법은 Gumbel[2], Frechet[3], Weibull[4] 분포의 일반화된 형태이므로 분포의 형태에 대한 다양한 설명이 가능합니다. 이를 통해 다양한 분포의 개형에 대한 접근이 가능합니다.

이에 반해 POT는 데이터 구간 내에서 임계값을 설정한 뒤 임계값 이상의 구간에 대한 데이터를 분석하는 기법입니다. POT에서 사용하는 Generalized Pareto Distribution의 방법은 Pickand–Balkema–de Hann 정리를 만족할 경우 이용할 수 있으며, 단변량의 임계값 이상의 데이터에 대한 모델링 능력이 뛰어납니다.

각 두 모델은 다음의 차이가 있습니다.

1. 첫번째로, 데이터 사용의 효율성 측면입니다. Block Maxima 방법을 사용하여 극값만을 찾는 것과는 다르게 POT는 임계값 이상의 모든 데이터를 사용해서 극단치를 모델링하므로 극값을 추정하는데 있어 더 많은 데이터 가용성이 있습니다. 이런 차이는 Block Maxima로 하여금 손실의 “최대규모”를 POT로 하여금 “규모”와 “빈도”를 추정하기 용이하도록 해줍니다.

2. 두번째로, 임계값의 설정 측면입니다. Block Maxima가 극단값만을 고려하기 때문에 분포의 유형이나 성격에 따라 다른 접근이 어려운 반면, POT는 성격에 따른 임계값 조정을 통해 예측 모형의 적합도를 개선할 수 있습니다. 이는 다양한 케이스의 가상자산간 관계들을 분석하는데 용이합니다.

1 CDF == $F(x;\mu,\sigma,\xi)=\exp(-[1+\xi(\sigma x-\mu)]^{-1/\xi})$

2 Gumbel 분포의 경우 ($\xi = 0$) 꼬리값이 지수적으로 감소하는 분포, 중간 수준의 극단치 데이터 분석에 적합

3 Frechet 분포의 경우 ($\xi > 0$) 꼬리가 무거워 극단적인 최댓값이 빈번하게 발생하는 데이터 분석에 적합

4 Weibull 분포 ($\xi < 0$) 꼬리가 얇아져 최대값이 한계값에 수렴하는 최대값이 빈번하게 발생하는 데이터 분석에 적합

이런 특징들은 Block Maxima로 하여금, 극단 피해수준에 대한 예측 POT는 Block Maxima가 예측하기 어려운 빈도와 규모를 추정할 수 있도록 해주므로 신용리스크 문제에 대해서 효과적으로 접근할 수 있도록 합니다.

2) Pickands-Balkema-de hann v. T-Copula

- **Pickands-Balkema-de Hann**

일반화된 파레토 분포의 경우, X가 확률분포함수 F(x)를 가진 상호 독립이며 동질적인 분포를 따르는 손실인 경우 및 u가 X의 임계치라고 할 경우, 임계치를 초과하는 극단치의 분포는 아래와 같이 표현됩니다.

$$F_u(X) = P(X \leq u + x \mid X > u) = \frac{F(x+u) - F(u)}{1 - F(u)}, x > 0$$

위의 식은 임계치를 초과하는 극단치에 대해 손실이 임계치를 x만큼 초과할 확률을 의미합니다. 여기서 임계치인 u값이 커질 경우 Pickands-Balkema-de Haan 정리에 따라서 아래와 같은 형태의 파레토 분포로 수렴합니다.

$$G_{\varepsilon,\vartheta}(X) = \begin{cases} 1 - (1 + \frac{\varepsilon x}{\vartheta})\text{^}(-\frac{1}{\varepsilon}) & if \quad \varepsilon \neq 0 \\ 1 - \exp(-\frac{x}{\vartheta}) & \quad\quad \varepsilon = 0 \end{cases}$$

임계치의 값이 충분히 크다고 가정할 경우 이에 따라 GPD의 적용이 가능합니다. 그에 따라 임계치의 하한과 상한을 벗어나는 극단적인 손실 범위를 제외한 보험료 산정이 가능합니다.

위의 논리에 따라 다음의 식이 도출될 수 있습니다.

$$Insurance\ Fee\ = \begin{cases} 0 & if\ 0 < X_i < r, \\ X_i - r & if\ r \leq X_i < R \\ R - r & if\ R \leq X_i < \infty \end{cases}$$

각 구간에 따라 Lending에 따른 특수 상황 발생시 책임 한도가 달라집니다. 임계치의 하한은 r이고 임계치의 상한은 R이 됩니다. 임계치를 초과하는 부분에 대해 채권을 풀링하여 CDS를 구매한 자들에게 본 리스크가 전가되며 차입/대출자 수수료와 CDS 수수료의 합에서 분배하여 가져가는 구조가 됩니다.

▪ T-Copula

T-Copula는 Pickands-Balkema-de Hann 정리와 같이 극단치 데이터를 분석하는 모델로, 균일한 분포를 따르는 확률변수들간의 결합분포를 만들어 변수간 의존성을 모델링하는데 사용됩니다. 특정 자산군의 리스크 분석에 있어 위험자산 포트폴리오는 통상 꼬리부분이 두꺼운 fat-tail한 양상을 보입니다. 이런 fat-tail한 형태를 띄는 분포에 대한 VaR 추정은 이런 형태의 분포는 실제 위험을 과소평가하는 문제를 발생시킵니다.

Copula 방식을 적용할 경우 개별 위험자산을 정규분포가 아닌 Extreme Value로 가정하며, 다변량 극단치 분포를 Copula 함수로 정의하므로, 실제 위험자산의 손실분포와 근사한 분산을 구할 수 있습니다.

T-Copula의 장점은 Pickands Balkema-de Hann이 단변량의 극단치 데이터 분석을 넘어서서 다변량 데이터의 변수간 의존성을 확인할 수 있다는 점입니다.

Bitinsurance는 위에서 설명한 Block Maxima, Peak over threshold Theory상 T-Copula를 통해 보험모델을 구현합니다. 개별 비트코인 및 bitRC-20 기반 토큰의 과거 가격 변동데이터를 수집하여 EVT를 적용하고, 그 상관관계 등에 대해 T-Copula를 적용합니다. 위를 통해 설정된 상당금액은 보험료 산정의 기본이 됩니다.

▪ BitInsuracne (CDS, Credit Default Swap)

bitSmiley는 독특한 포인트는 위의 Lending Protocol에서 발행된 대출건들에 대한 보험채권을 풀링하여 CDS 형태의 채권으로 형성한 뒤 재판매한다는 점입니다. 발행된 CDS를 여러 NFT로 분할하여 제 3자에게 매각하는 방식으로 복잡한 보험 사무를 대리합니다. 발행된 CDS에 대한 보상은 채무 불이행률을 근거로 계산되며, 채무 불이행률의 구간에 따라 일정 비율 미만의 채무 불이행률을 기록할 경우 CDS의 구매자가 그에 대한 보상을 받아가는 구조입니다.

이런 CDS의 가격 결정은 입찰의 방식을 통해서 개별 라운드를 진행하고 이에 따라 낙찰된 금액을 기준으로 설정됩니다.

2) Technical Details

bitSmiley의 주요한 서비스인 bitUSD/bitLending을 구현하기 위해서 반드시 필요한 것은 다음과 같습니다.

① The Indexer to fetch proper off-chain price data or on-chain data

② The Validator to verify data fetched by Indexer

③ DAO to validate bitRC-20-related activities

④ The Relayer to record bitSmileyDAO consensus results

Definition

▪ Indexer & Validator

Indexer는 통상 블록체인 상에서 외부 가격 데이터를 받아오는 자를 말합니다. 하지만 오디널스 기반의 Indexer는 그 성격에 차이가 있습니다. 비트코인은 이더리움과 같이 계정 기반의 상태변화를 지원하지 아니하므로, 온체인상 전체 잔액의 상태를 파악하기 어렵다는 한계를 갖습니다. 따라서 BitSmiley상의 Indexer의 기능은 "BitRC-20의 온체인 상의 상태"와 "오프체인 상의 가격데이터"를 받아오는 것입니다.

Indexer가 데이터를 받아서 Protocol 상에 업데이트 한다고 하더라도 이에 대한 자료의 적절여부를 판단할 필요가 있습니다. 플랫폼 상에서 Validator는 데이터의 적정 여부를 검증하는 역할을 수행합니다.

Relayer

Relayer는 BitSmiley 플랫폼 상의 합의 결과를 Bitcoin 블록체인에 기록하는 기능을 수행합니다.

Voting Contract & Oracle Contract

Indexer와 Validator로부터 제출된 데이터를 SmileyDAO에 제출하는 역할을 수행합니다.

bitSmileyDAO

bitSmileyDAO는 bitSmiley 플랫폼과 관련되어 1) 주요 정책의 결정 2) bitRC-20의 최종 검증 등을 수행합니다. 주요 정책의 결정 예시로는 단위 비트코인에 대하여 BitUSD의 발행량을 결정하거나, 청산가격을 설정하는 등의 플랫폼 주요 의사결정에 관여합니다. 또한 bitUSD의 발행 등의 과정에서 주요 검증자로 참여하여 bitSmileyDAO의 투표를 통해 플랫폼 상에 발생할 수 있는 외부 리스크 발생 시 "Emergency Shutdown Mechanism"과 이를 재개할 수 있는 "Economic Governance Committee" 관리의 주체가 됩니다.

bitRC-20

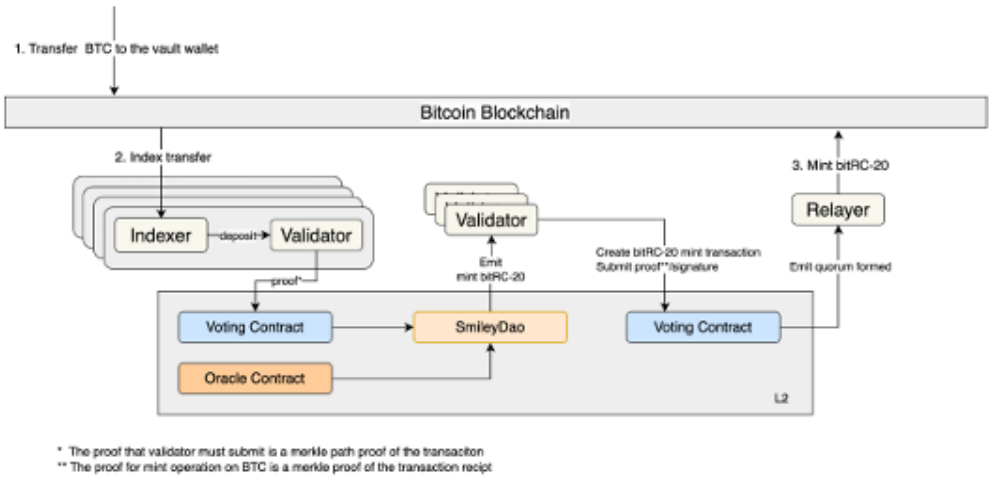
bRC-20 인스크립션 내용

```
{
    "p": "bitRC-20",
    "tick": "bitUSD",
    "op": "deploy",
    "init": "21000000",  // the initial token amount
    "dec": 18,
    "v": 1,              // the version number
    "scripts": {
        "mint": "hash256 or empty",
        "burn": "hash256 or empty",
        "transfer": "hash256 or empty"
    }
}
```

bitSmiley가 제안하는 인스크립션 프로토콜로 JSON의 구조입니다. 상기 코드에서 “p”는 프로토콜 “tick”은 발행자산의 티커, “op”는 활동명, “init”는 발행 토큰의 수량, “dec”는 소수점, “v”는 버전명, “Script”는 지원하는 스크립트의 명칭을 말합니다.

bitRC-20 Process

bitRC-20 발행 절차



bitRC-20의 발행과정은 위와 같습니다. (bitUSD 포함)

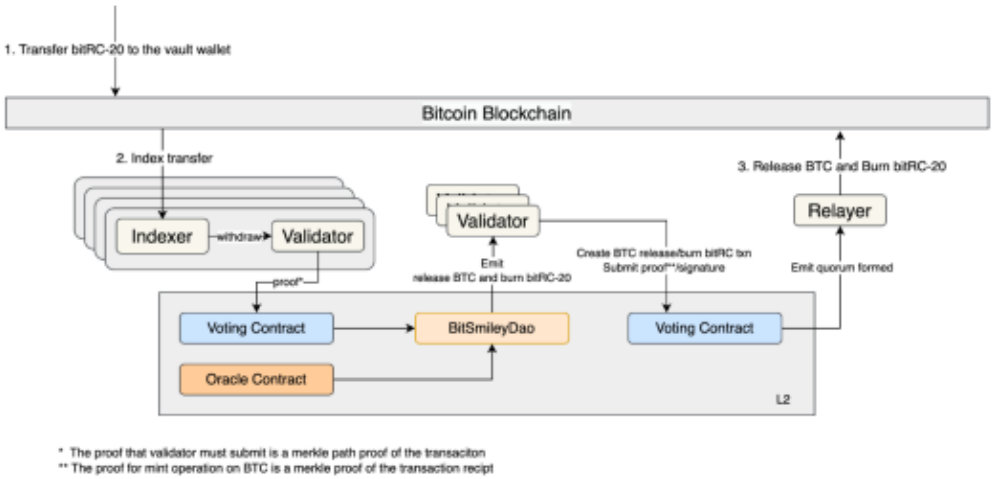
1) 비트코인을 비트코인 네트워크 상 bitSmiley 볼트에 입금

2) 비트코인의 Vault 입금을 Indexer가 확인하고, “입금 사실”을 Validator에 제출

3) 제출된 트랜잭션을 Oracle Contract와 Voting Contract를 통한 DAO 데이터 검증진행

4) SmileyDAO는 제출받은 자료를 바탕으로 bitRC-20 트랜잭션을 실행하고 릴레이어를 통해 bitRC-20 토큰을 발행

bitRC-20 소각 절차



bitRC-20 소각 절차는 위와 같습니다. (bitUSD 포함)

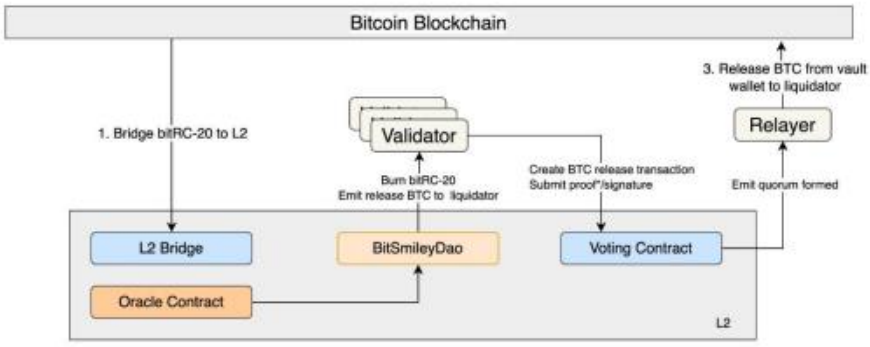
1) bitRC-20 Token을 비트코인 네트워크 상 bitSmiley 볼트에 입금

2) bitRC-20 Token의 Vault 입금을 Indexer가 확인하고, “출금 사실”을 Validator에게 제출

3) 제출된 트랜잭션을 Oracle Contract와 Voting Contract를 통한 DAO 데이터 검증진행

4) SmileyDAO는 제출받은 자료를 근거로 bitRC-20 트랜잭션을 실행하고 릴레이어를 통해 Burn 사실을 기록

비트코인 청산 절차



bitUSD의 청산 절차는 위와 같습니다.

1) 임계점에 도달한 bitUSD/Bitcoin 계약을 식별
2) 관련 내용을 Oracle을 통하여 SmileyDAO로 제출
3) BitSmileyDAO는 식별한 담보 BTC를 릴레이어를 통해 Liquidator에게 전송
4) Liquidator에 의한 청산절차 진행

Emergency Shutdown Mechanism

bitSmiley가 가지고 있는 독특한 기능은 Emergency Shutdown Mechanism(이하 “ESM”)입니다. ESM은 시스템에 대한 공격 혹은 보안상의 문제가 발생했을 경우 발동합니다. ESM의 주체는 SmileyDAO에 포함된 Economic Governance Committee로 다음 4단계로 시행됩니다.

1. 비상상황 발생시 플랫폼의 폐쇄
   Shutdown 결정이 발효된 직후 오라클은 정지하며 각 사용자는 부채를 상환할 수 있는 정도의 담보만 인출할 수 있습니다.

2. 경매 매커니즘의 활성화
   ESM은 담보물에 대한 경매를 발효하여 시스템 내의 부채를 상환을 실시합니다.

3. 남은 담보의 상환
   경매가 종료된 직후, bitUSD 보유자는 고정된 비율로 담보를 회수할 수 있습니다.

4. 플랫폼 재시작
   앞의 3단계가 시행된 이후 Economic Governance Committee의 결정에 따라 플랫폼이 재시작 됩니다.

모든 bitSmiley에서 이루어지는 활동은 DAO를 경유하여 승인이 발생하고 릴레이어를 통해 기록되므로, Economic Governance Committee는 플랫폼에 대한 공격을 손쉽게 대응할 수 있습니다.

Ⅳ. Examination of bitSmiley

bitSmiley에 Lightning Network를 적용할 수 있는지 여부에 대한 검토

상기 언급한 바와 같이 bitSmiley에서의 중요한 문제는 Settlement까지의 시간입니다. bitSmiley는 Inscription 기반이기 때문에 실행된 조건문이 비트코인 개별 블록에 등록될 때까지 체결이 지연되게 됩니다. Lightning Network의 경우 오프체인 방식으로 간소화된 채널을 이용하여 HTLCs 방식으로 비트코인의 결제를 수행합니다.

bitSmiley는 Indexer와 Validator 그리고 SmileyDAO, Relayer 의사결정을 경유하여 개별 활동이 집계되고 승인되어 처리되는 방식입니다. HTLCs를 사용하는 Lightning Network의 개별 망이 smileyDAO에 연동되지 않는 이상 오프체인 방식과는 호환되기 어렵고, 특히 Relayer를 통해 온체인에 기록되는 SmileyDAO의 방식으로는 Lightning Network과의 호환은 상상하기 어렵습니다.

bitSmiley의 중앙화 문제 검토

이더리움의 MakerDAO의 거버넌스 시스템이 MKR 홀더에 의해서 결정되는 방식과는 다르게 bitSmiley의 거버넌스는 내부적으로 선정된 DAO의 Committee에 의해서 중요한 정책이 결정되게 됩니다. 특히 Shutdown 시스템과 같은 기능은 탈중앙화 된 조직의 취지와 다르며 또한 프로토콜 기반이 아닌 정성적인 요인들이 개입할 수 있습니다.

하지만 MakerDAO의 MKR은 담보대출과 관련된 결정 부분에서 청산리스크를 부담하므로 지표 결정에 대한 견제의 강점은 있으나, MKR의 단기적 매수 매도를 통해 의사결정에 개입할 수 있다는 점 및 이를 통해 Liquidation Ratio 등에 대해 이해관계에 따라 조정할 수 있다는 문제를 갖고 있습니다. 이는 경우에 따라 투기적 소요에 이더리움 생태계를 노출시켜, 큰 변동성을 야기할 수 있습니다.

만일, bitSmiley의 개별 플레이어가 소수로 구성되지만, 청산 등의 리스크를 충분히 견제할 유인이 존재할 수 있다면 위의 성격에서 신속한 의사결정 및 더 효율적인 서비스의 유지관리를 가능케 할 수 있습니다.

bitSmiley의 CDS 판매 가능성 검토

bitSmiley은 다른 플랫폼에서 시도해보지 않은 Lednding의 보험상품과 개별 채권을 풀링한 CDS 서비스를 제공합니다. 위 서비스는 Lending 과정에서 발생한 채권을 풀링하여 제 3자에게 매각한 뒤, 신용리스크를 제 3자가 일부 전가하는 방식입니다. 하지만 과거에 블록체인 기반 P2P Lending Platform들의 통상적인 문제에서 발견되었듯, 차입자의 신용이 명확하게 평가되지 않을 경우 상환 불능의 위험이 있습니다. 특히 Pool 기반이 아닌 P2P 기반의 Lending Platform은 범지구적인 형태의 계약이 이루어지기 때문에, 상환불능에 대해 압류/경매 등을 통해 회수를 강제할 수 없는 한계가 있습니다. 뿐만 아니라, 가상자산 시장은 급격한 가격변동에 노출되어 있으므로, CDS의 적절한 수수료율을 계산할 수 있는지 여부는 미지수입니다.

이런 경우 솔루션은 크게 두가지입니다.

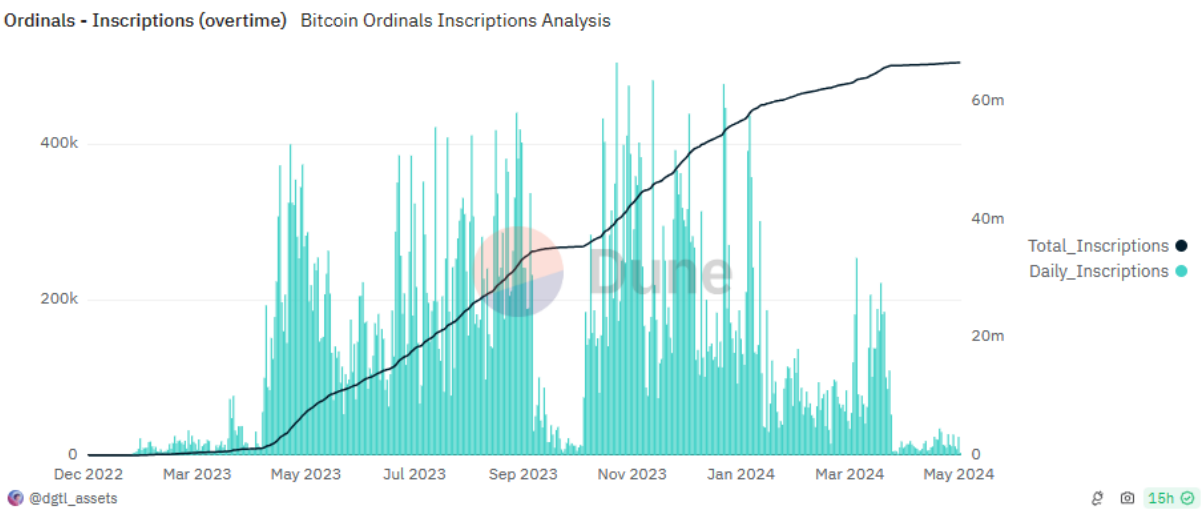
첫번째는 Wallet의 KYC/AML 등을 통하여 Wallet의 소유주를 식별하고, SmileyDAO에 전세계에 채권을 관리할 수 있는 회사를 배정하여 채권관리 수수료를 지급하는 방법입니다. 하지만 본 건의 경우 채권관리 수수료가 상당하고, 회수까지의 상당 시간이 소요되며, 차입자에게 상환을 요구할 수 있는 자산이 없을 경우 대손으로 식별된다는 점입니다. 위와 같은 리스크가 CDS에 반영될 경우 채권의 가격 자체가 심각하게 저평가되어 실질적인 보험으로의 기능을 수행하기 어려울 수 있습니다. 또한 부가적으로 탈중앙화와 다르게 개인을 식별할 수 있다는 점은 서비스 측면에서의 단점이 됩니다.

두번째는 Liquidation Ratio를 높이는 방법입니다. 담보된 자산이 청산되는 가격한도를 높일 경우, 실제 경매로 이어짐에 따라 Liquidator와 bitSmiley Pool에 쌓이게 되는 담보 자산의 규모가 증가하게 됩니다. 하지만 이렇게 될 경우, bitsmiley의 담보 대출 프로토콜은 타 서비스에 비해 높은 Liquidation Ratio를 가지게 되고 DEFI 등의 서비스 이용 관점에서 승수 효과가 줄어듭니다. 이는 bitSmiley 선택의 요인을 낮추고, bitSmiley의 초기 Pool 형성의 제약이 됩니다.

물론 그럼에도 불구하고, bitSmiley측에서 충분한 유동성을 바탕으로 Lending등의 풀을 형성하고 bitRC-20 기반 토큰의 담보 Lending시 제한을 명확하게 제안, 및 이에 대한 CDS 인수 등을 수행하는 등의 자기자본을 이용한 불확실성 감소를 수행한다면 일정 부분 해결될 수 있는 문제일 수 있습니다.

V. Conclusion (프로젝트에서 주목할만한 포인트)

오디널스 발행 현황



초기 인스크립션의 등장 이후 평균 10만개 수준의 인스크립션들이 발행되어 왔습니다. 인스크립션이라는 행위가 단순히 블록에 특정 코드를 기록하는 행위라고 하더라도, 비트코인을 통한 실험적인 시도는 흥미롭습니다.

마찬가지로 Stacks와 같은 레이어2 프로젝트가 아닌, 인스크립션만을 이용하여 비트코인 자체망에서 DEFI의 솔루션을 제안하는 것은 비트코인 유저들에게 새로운 실험적 시도가 될 수 있습니다. 뿐만 아니라 bitUSD를 이용한 거래시장을 충분히 형성할 경우, 보유하고 있는 대량의 비트코인을 시장에서 매도하지 아니하고서도 비트코인 블록체인 내에서 유동화 등의 솔루션으로 기능할 수 있습니다.

구체적으로 다음의 특이점들이 있습니다.

1. bitSmiley는 비트코인의 보안성을 이용하여 프로토콜을 운영한다는 점에서 강점이 있습니다. 하지만, 속도 부분과 확장성 부분에 한계가 있습니다. 기관 등의 대량 자금 이동에 유용합니다.

2. Bitcoin 기반의 프로토콜로 비트코인을 유동화 할 수 있다는 점에서 강점을 갖습니다. 현재 유통되는 비트코인을 매도하기 위한 장내 유동성이 충분하지 않다는 점에서, bitUSD를 이용한 거래 방식은 bitUSD를 통한 충분한 거래채널을 보유할 경우 유효합니다.

3. CDS 방식의 풀링 서비스는 이를 기반으로 하는 새로운 상품 개발을 가능하게 만들 수 있습니다.

4. bitSmiley는 오디널스의 특성상 Peer to Peer로 거래됩니다. 유동성이 Pool 형태로 조성되지 못하고 파편화 되어 있으므로 대여자 또는 대출자 간의 매칭에서 한계를 갖습니다. 하지만, 타 플랫폼과 다른 고이율을 원하는 플레이어를 위한 대출 플랫폼이 될 수 있습니다.